

An identity for the Kloosterman sum

D. I. Tolev

Abstract

We establish a simple identity and using it we find a new proof of a result of Kloosterman.

Keywords: Kloosterman sums; MSC 2010: 11L05, 11L07.

The Kloosterman sum is defined by

$$K(p; a, b) = \sum_{x=1}^{p-1} e_p(ax + b\bar{x}), \quad (1)$$

where p is a prime, a and b are integers, \bar{x} is the inverse of x modulo p and $e_p(\alpha) = \exp\left(\frac{2\pi i \alpha}{p}\right)$. It is clear that it takes always real values. This sum was introduced in 1926 by Kloosterman [1] and he established that

$$|K(p; a, b)| \leq 3^{1/4} p^{3/4} \quad \text{for} \quad p \nmid ab. \quad (2)$$

In 1948 A.Weil [6] improved substantially the estimate (2) and obtained the following deep and important inequality:

$$|K(p; a, b)| \leq 2\sqrt{p} \quad \text{for} \quad p \nmid ab. \quad (3)$$

Later Stepanov [5] found an elementary proof of (3) (see also Iwaniec and Kowalski [4], Chapter 11). Information about the applications of Kloosterman's sum in analytic number theory as well as a simple proof of (2) can be found in Heath-Brown's paper [3]. Another proof of (2) is available in the recent preprint [2] from Fleming, Garcia and Karaali.

In this short note we present an identity for the Kloosterman sum and using it we find a new proof of (2) (with smaller constant in the right-hand side of this inequality).

From this point onwards we assume that $p > 2$ is a fixed prime and let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. We write for simplicity $K(a, b) = K(p; a, b)$. Our result is the following

Theorem. For any integers a, b such that $p \nmid ab$ we have

$$K(a, b)^2 = p + \sum_{l=1}^p \left(\frac{l^2 - 4l}{p} \right) K(a, lb). \quad (4)$$

Proof: Using (1) we find

$$\begin{aligned} K(a, b)^2 &= \sum_{1 \leq x, y \leq p-1} e_p(a(x-y) + b(\overline{x} - \overline{y})) = \sum_{h=1}^p e_p(ah) \sum_{\substack{1 \leq x, y \leq p-1 \\ x-y \equiv h \pmod{p}}} e_p(b(\overline{x} - \overline{y})) \\ &= p - 1 + Y(a, b), \end{aligned} \quad (5)$$

where

$$Y(a, b) = \sum_{h=1}^{p-1} e_p(ah) \sum_{\substack{1 \leq y \leq p-1 \\ p \nmid y+h}} e_p(b(\overline{y+h} - \overline{y})).$$

We put $y = hz$ in the inner sum and obtain

$$Y(a, b) = \sum_{h=1}^{p-1} e_p(ah) \sum_{z=1}^{p-2} e_p(b\overline{h}(\overline{z+1} - \overline{z})).$$

Now we change the order of summation and use (1) to get

$$Y(a, b) = \sum_{z=1}^{p-2} K(a, b(\overline{z+1} - \overline{z})) = \sum_{l=1}^{p-1} K(a, lb) \lambda_l, \quad (6)$$

where λ_l is the number of integers z such that $1 \leq z \leq p-2$ and $\overline{z+1} - \overline{z} \equiv l \pmod{p}$.

We easily see that λ_l equals the number of solutions of the congruence $lz^2 + lz + 1 \equiv 0 \pmod{p}$, hence from the properties of the Legendre symbol it follows that

$$\lambda_l = 1 + \left(\frac{l^2 - 4l}{p} \right). \quad (7)$$

From (1) and our assumption $p \nmid ab$ we get

$$\sum_{l=1}^{p-1} K(a, lb) = \sum_{x=1}^{p-1} e_p(ax) \sum_{l=1}^{p-1} e_p(bl\overline{x}) = - \sum_{x=1}^{p-1} e_p(ax) = 1. \quad (8)$$

The identity (4) is a consequence of (5) – (8). □

Now we obtain immediately the following

Corollary. *If $p \nmid ab$ then*

$$|K(a, b)| \leq \sqrt{p + p^{3/2}}. \quad (9)$$

Proof: Denote by Z the second term in the right-hand side of (4). From Cauchy's inequality we get

$$|Z| \leq p^{1/2} \left(\sum_{l=1}^p K^2(a, lb) \right)^{1/2} = p^{1/2} Z_1^{1/2},$$

say. From (1) it follows that

$$Z_1 = \sum_{1 \leq x, y \leq p-1} e_p(a(x-y)) \sum_{l=1}^p e_p(bl(\bar{x} - \bar{y})) = p(p-1).$$

Hence $|Z| \leq p^{3/2}$ and using (4) we obtain (9). □

Finally we mention that by the same method we can estimate also the sum

$$K_r(p; a, b) = \sum_{x=1}^{p-1} e_p(ax^r + b\bar{x}),$$

for arbitrary positive integer r . We can prove that $K_r(p; a, b) \ll_r p^{3/4}$ for $p \nmid ab$, but we shall not give the details here.

Acknowledgments: The present research was supported by Sofia University Grant 172/2010.

References

- [1] H.D.Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$* , Acta Mathematica, 49, (1926), 407–464.
- [2] P.S.Fleming, S.R. Garcia, G.Karaali, *Classical Kloosterman sums: representation theory, magic squares, and Ramanujan multigraphs*, arXiv:1004.3550.
- [3] D.R.Heath-Brown, *Arithmetic applications of Kloosterman sums*, NAW, 5/1, 4 (2000), 380–384.
- [4] H.Iwaniec, E.Kowalski, *Analytic number theory*, Colloquium Publications, vol. 53, Amer. Math. Soc., 2004.

- [5] S.Stepanov *An estimation of Kloosterman sums*, Izv. Akad. Nauk SSSR Ser. Mat., 35, (1971), 308-323
- [6] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204-207.

Faculty of Mathematics and Informatics
Sofia University “St. Kl. Ohridsky”
5 J.Bourchier, 1164 Sofia, Bulgaria

Email: dtolev@fmi.uni-sofia.bg